Electromagnetic Analysis Perturbation using Chaos Generator

Thomas Sarno, Romain Wacquez,Edith Kussener, Philippe Maurine, Khalil Jradi, Jean-Michel Portal, Driss Aboulkassimi, Sarra Souiki-Figuigui, Jeremy Postel-Pellerin, Pierre Canet, Maxime Chambonnea, David Grojo

***Abstract*—Cryptographic algorithms albeit mathematically sure may have security breaches when implemented on hardware chips. There are several ways to compromise their security, one method is to analyze their electromagnetic (EM) emissions in order to find secrets (cryptographic keys for example). This paper proposes a proof of concept of a countermeasure against these attacks, it is based on a chaotic oscillator coupled with an antenna to blur the EM emissions of the chip. The objective is to generate EM noise within the chip with an internal system in order to make the secret information harder to extract. A testchip was developed and tested in conditions as close as possible to real use-case to prove the relevance of the concept. The EM field collected while running the chip were superposed to AES (Advanced Encryption Standard) emissions collected using a similar setup to test the disturbing effect of the noise on a CPA, a classic attack to retrieve AES keys. The experiment shows that it can effectively increase the difficulty of finding the keys, proving that the basic concept and the developed chip can be used as a countermeasure for EM analysis attacks.**

I. Introduction

This study proposes a countermeasure concept based on coupling a cryptographic chip with a chaotic EM generator. It could prevent side-channel attacks relying on analysis of EM field.

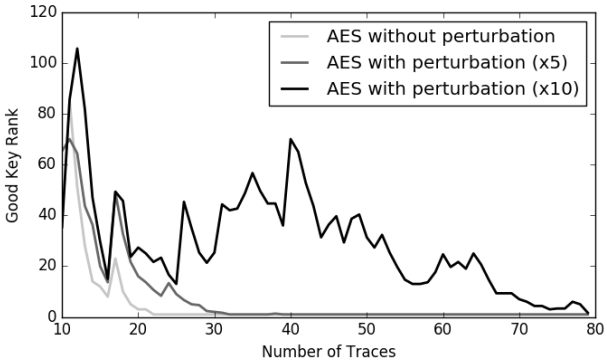
The circuit used is generating random EM emissions. It is based on a true random number generator (TRNG) using a discrete-time chaotic oscillator described in [1]. This method is low-power making it suitable for a built-in countermeasure. The chaotic nature of the output signal was well demonstrated as it passed the NIST randomness test suite [2] but the characteristic period of the oscillations was too high (from 500us to 5ms) to be realistically used against a cryptographic system typically running at tens of MHz.

II. EM Emissions from chaos generator

The prototype chip tested was designed without protections (ESD protection, insulating resin), therefore many precautions were needed not to damage it. In particular a safety distance between the EM probe and the chip antenna was necessary. It resulted on a reduction of the magnetic field collected and an important background noise. To tackle this issue, the raw measurements had to be processed to extract relevant data. These processing included the selection and the synchronizations of given patterns to see their EM signatures. It showed that the EM signature of some of these patterns had amplitudes of the order of typical signatures of cryptographic circuits.

The processing also showed that the amplitude of some patterns were variable, depending on the chaotic input. In these patterns, the chaotic nature of the signal was carried in their amplitude instead of their frequency allowing a use to perturb higher frequency signals. A realistic way to test the validity of our method is to superpose the cryptographic signatures and the chaotic signatures and use cryptanalysis methods to retrieve the key and see the effects of the perturbation.

The cryptographic traces used were measured on a software AES embedded in a 32bits micro-controller running at 50MHz, the attack is a CPA focusing on the subbyte operation of the algorithm.These traces were superposed with the variable amplitude patterns signatures. There were divided into eight groups with each a different amplitude and for each cryptographic traces one of these signature was randomly selected and superposed with a random time offset.



A multiplicative factor on the perturbation was set to simulate the fact that the EM measurement was attenuated due to distant constraints. The results presented above show a significant increase of the number of traces needed to retrieve the key. On this particular configuration the key is easily found even with the countermeasure but the perturbation it causes have a visible effect on the cryptanalysis which is likely to remain even on more resilient configuration (hardware implementation for example).

III. Conclusion and perspective work

The experiment is a proof of concept for the perturbation of cryptanalysis methods using this type of method. They show that despite the circuits running at different frequencies, the countermeasure is able to significantly increase the number of traces and therefore the time needed to retrieve the cryptographic key. Further experiment on other targets are being planned to confirm the viability of the concept. The objective is integrating both the cryptographic circuit and the countermeasure on a single chip to propose a built-in protection against EM cryptanalysis.

References

[1] E. Kussener J. A. Aguilar Angulo. Discrete chaos - based random number generator. In *Faible Tension Faible Consommation (FTFC), 2014 IEEE*.

[2] Lawrence E. Rukhin Bassham, III. Sp 800-22 rev. 1a. a statistical test suite for random and pseudorandom number generators for cryptographic applications. Technical report, 2010.